



## *Furto di identità*

### *Conoscere i fatti*

Al giorno d'oggi bisogna prestare particolare attenzione al proteggere la propria identità.

I ladri di identità rubano dati identificativi personali, tra cui il numero di previdenza sociale (social security number) e i numeri dei conti bancari e delle carte di credito, dati, cioè, che possono essere utilizzati per ottenere crediti, effettuare acquisti e persino stipulare polizze assicurative a nome della vittima. I risultati possono essere devastanti: fatture per migliaia di dollari a fronte di acquisti mai effettuati e una situazione creditizia rovinata il cui ripristino può richiedere mesi o anni.

I moderni ladri di identità inviano e-mail fraudolente presentandosi come aziende ed enti governativi legittimi, persino amici e parenti, per cercare di ingannare il consumatore affinché riveli informazioni identificative personali.

### *Proteggere la propria identità*

Ci sono diversi modi per proteggersi contro il furto dell'identità:

- Non comunicare mai informazioni identificative personali durante una telefonata non sollecitata o in risposta a un'e-mail ricevuta da una banca, da un amico o persino da un familiare senza prima contattare la fonte per confermare la legittimità del messaggio di posta elettronica e capire perché l'individuo o la banca richiede tali informazioni. Non fidarsi automaticamente dei numeri di telefono ricevuti in telefonate o e-mail non sollecitate, ma verificare in modo indipendente i numeri appropriati.
- Monitorare il proprio rapporto di credito: le leggi federali impongono alle tre principali centrali rischi di fornire una copia gratuita del rapporto di credito tutti gli anni. Richiedendo periodicamente la copia del proprio rapporto di credito dalle centrali rischi, è possibile assicurarsi che nessuno stia richiedendo a proprio nome carte di credito o prestiti.
- Non pubblicare mai online informazioni identificative personali, a meno che non si abbia buon motivo di ritenere che il sito Web è sicuro. Prima di effettuare un acquisto online con carta di credito, verificare l'identità, l'indirizzo reale e il numero di telefono del venditore in caso insorgano problemi relativamente alla vendita. Verificare la presenza di simboli che indicano che il sito Web è sicuro. Controllare se sono stati sporti reclami nei confronti del venditore. La FTC suggerisce quanto segue: "Se si riceve un'e-mail o un messaggio pop-up che domanda informazioni finanziarie mentre si naviga in rete, non rispondere e non seguire il collegamento. Le aziende legittime non richiedono informazioni in questo modo".
- Per evitare il malware, adottare misure come:
  - Non fare mai clic sui pop-up;
  - Non fare mai clic su collegamenti negli allegati a meno di essere sicuri che la fonte è affidabile;
  - Utilizzare software firewall, antivirus e antispyware e aggiornare regolarmente il software e
  - Spiegare ai propri figli come comportarsi online per non creare problemi di sicurezza.
- Strappare i documenti che contengono informazioni identificative personali prima di gettarli.
- Non portare nel portafoglio la tessera della sicurezza sociale.
- Utilizzare password univoche e forti per tutti gli account di Internet e modificarle periodicamente. Non condividere mai le password.



### Furto di identità

#### Nel caso si fosse una vittima di furto di identità

- Contattare le banche e le emittenti delle carte di credito.
- Inserire un avviso di frode e/o un più rigoroso “blocco di sicurezza” sul proprio rapporto di credito.
  - A tal fine si può contattare una delle principali centrali rischi che provvederà ad avvertire le altre due. Una volta inserito, l’avviso impone a qualsiasi azienda di verificare l’identità dell’utente prima di emettere una carta di credito. Gli avvisi di frode sono gratuiti e rimangono in vigore per 90 giorni a meno che non vengano rinnovati.
  - Se si preferisce inserire il più rigoroso blocco di sicurezza sul proprio rapporto di credito, è necessario contattare singolarmente tutte e tre le centrali rischi. Anche se le centrali rischi possono addebitare un costo per l’inserimento e la rimozione dei blocchi di sicurezza, una volta attuato, le centrali dei crediti non possono comunicare le informazioni del soggetto senza autorizzazione esplicita.
- Sporgere denuncia presso la polizia. Le leggi del Connecticut consentono alle vittime di furti di identità di segnalare il furto stesso alle forze dell’ordine nel luogo di residenza e ottenere una copia della denuncia.
- Se le informazioni personali sono state compromesse on-line, rivolgersi all’Internet Crime Complaint Center (centro per le denunce dei crimini Internet) sul sito: [www.ic3.gov](http://www.ic3.gov).

#### Risorse

- Per ottenere copie gratuite del proprio rapporto di credito dalle tre principali centrali rischi, scrivere a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Ricordarsi di precisare la centrale rischi da cui si desidera ottenere il rapporto, oppure utilizzare il modulo disponibile presso il sito <http://www.consumer.ftc.gov/articles/0155-free-credit-reports>. Si può anche visitare il sito [www.annualcreditreport.com](http://www.annualcreditreport.com) o telefonare al numero 1-877-322-8228.
- Le tre centrali rischi forniscono rapporti di credito annuali a titolo gratuito **esclusivamente** tramite [annualcreditreport.com](http://www.annualcreditreport.com), il numero 1-877-322-8228 o per posta inviata ad Annual Credit Report Request Service.
- Si possono contattare direttamente le tre centrali per questioni diverse dalla richiesta di un rapporto gratuito servendosi delle seguenti informazioni:

Equifax  
1-888-766-0008  
[www.equifax.com](http://www.equifax.com)

Experian  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
1-800-888-4213  
[www.transunion.com](http://www.transunion.com)

- Si può inoltre inviare reclamo all’ufficio dell’Attorney General (Procuratore generale) compilando un modulo di reclamo sul sito [www.ct.gov/ag](http://www.ct.gov/ag).